Volume 15, Issue 11 • Nov. 2020 | Monthly Security Tips Newsletter

What You Need to Know About Ransomware

From the desk of
Michael Aliperti
MS-ISAC Chair

What is Ransomware

Ransomware is a type of malicious software, or malware, that blocks access to a system, device, or file until a ransom is paid. It is an illegal, moneymaking scheme that can be installed through deceptive links in an email message, instant message, or website.

Ransomware works by encrypting files on the infected system (crypto ransomware), threatening to erase files (wiper ransomware), or blocking system access (locker ransomware) for the victim. The ransom amount and contact information for the cyber threat actor (CTA) is typically included in a ransom note that appears on the victim's screen after their files are locked or encrypted.

Sometimes the CTA only includes contact information in the note and will likely attempt to negotiate the ransom amount once they are contacted. The ransom demand is usually in the form of cryptocurrency, such as Bitcoin, and can range from as little as several hundred dollars up to and exceeding one million dollars. It is not uncharacteristic to see multi-million-dollar ransom demands in the current threat landscape.

Ransomware is primarily delivered through the following means:

- Malicious attachments/links sent in an email.
- Network intrusion through poorly-secured ports and services, such as Remote Desktop Protocol (RDP) (e.g. Phobos ransomware variant).
- Dropped by other malware infections (e.g. initial TrickBot infection leading to a Ryuk ransomware attack).
- Wormable and other forms of ransomware that exploit network vulnerabilities (e.g. the WannaCry ransomware variant).

Why is Ransomware Awareness Important?

Ransomware is a growing and expensive problem. In 2019, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed a 153% increase in the number of reported state, local, tribal, and territorial (SLTT) government ransomware attacks from the previous year. Many of these incidents resulted in significant network downtime, delayed services to constituents, and costly remediation efforts.

Victims of ransomware are not only at risk of losing access to their systems and files. In many cases, they may also experience financial loss due to legal costs, purchasing credit monitoring services for employees/customers, or ultimately deciding to pay the ransom. The effects of a ransomware attack are particularly harmful when it impacts emergency services and critical infrastructure, such as 911 call centers and hospitals.

Additionally, CTAs target managed service providers (MSPs), a company that manages a customer's Information Technology (IT) infrastructure, to push out ransomware to multiple entities. This occurs when CTAs compromise an MSP and use their existing infrastructure to disseminate the ransomware to the MSP’s clientele. This exploits the trusted relationship between the customer and their MSP.

Over the past few years, the MS-ISAC observed an increase in means that allow CTAs to evade detection and maximize the impact of their attacks. One such means includes what is called “living off the land” (LOTL): deploying publicly-available penetration testing suites or tools (e.g., Cobalt Strike, Metasploit, or Mimikatz), to specifically target domain controllers and Active Directory to gain network wide access and deploy fileless ransomware to evade any signature-based antivirus.

What Can You Do About Ransomware?

Defending against ransomware requires a holistic, all-hands-on-deck approach that brings together your entire organization. While ransomware infections are not entirely preventable due to the effectiveness of well-crafted phishing emails and drive-by downloads from otherwise legitimate sites, organizations can significantly reduce the risk of ransomware by implementing cybersecurity policies and procedures and improving cybersecurity awareness and practices of all employees.

It is up to all of us to help prevent ransomware from successfully infecting our systems. To increase the likelihood of preventing ransomware infections, organizations must implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. This program should include organization-wide phishing tests to gauge user awareness and reinforce the

importance of identifying potentially malicious emails. When employees can spot and avoid malicious emails, everyone plays a part in protecting the organization.

If your organization becomes infected with ransomware, there are some things you can do to respond. The most effective strategy to mitigate the risk of data loss resulting from a successful ransomware attack is having a comprehensive data backup process in place; however, backups must be stored off the network and tested regularly to ensure integrity.

Reporting Ransomware

If your organization is the victim of a ransomware infection, follow your organization's incident response procedures to report it. Alternatively, the Cybersecurity and Infrastructure Security Agency (CISA) provides a secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To submit a report, visit https://us-cert.cisa.gov/report.